	Georgia Technology Authority	
Title:	**Disaster Recovery – System Backups**	
PSG Number:	SS-08-046.01	**Topical Area:** Security
Document Type:	Standard	**Pages:** 2
Issue Date:	3/31/08	**Effective Date:** 3/31/08
POC for Changes:	GTA Office of Information Security	
Synopsis:	Establish requirement to establish backup and recovery procedures for critical software and data.	

PURPOSE

System backups are an essential component of contingency planning strategies. Backups enable IT support personnel to quickly and reliably recover essential data and software in case of events such as natural or environmental disasters, system or application failures, sabotage, data/system integrity errors and/or system operations errors.

This standard establishes the minimum requirements for agencies to create procedures for the backup, storage and recovery of critical information systems, applications and data as part of their contingency planning strategy.

SCOPE; ENFORCEMENT; AUTHORITY; EXCEPTIONS

See Enterprise Information Security Charter (policy)

STANDARD

Each agency's IT contingency planning /disaster recovery strategy shall include detailed and documented procedures for back-up, storage and restoration of operationally critical hardware, software and data.

Agencies' backup and recovery procedures shall include but are not limited to the following:

- Step-by-step system/data restoration and/or alternate processing procedures based on availability and integrity requirements.
    - The maximum elapsed time that a critical function or service can be inoperable without a catastrophic impact to that function or service.
    - The maximum amount of information or data that can be lost without a catastrophic impact to a critical function or service.
- Backup schedules (e.g., daily or weekly, incremental or full) - based on data

criticality and the frequency that data changes.
- Storage and location of backup media - shall be in a physically and environmentally secure location and adequately labeled to ensure proper handling and prompt identification. Media for critical systems, applications and data shall be stored at a location remote from the main processing site.
- Procedures and chain of custody logs for transporting backup/storage media offsite in accordance with the Media Protection and Handling standard (if applicable).
- Media retention periods - shall be determined based on an evaluation of agency, state, federal and legal archive requirements and implications. Critical applications and data shall have a minimum of 3 full backup cycles readily available.
- Media and file-naming conventions.
- Media rotation frequency.

Backup media and restoration procedures shall be routinely tested to ensure data and systems can be reliably restored.

RELATED ENTERPRISE POLICIES, STANDARDS, GUIDELINES

- Business Continuity and Recovery (Policy)
- Contingency Planning (Standard)
- Media Controls (Policy)
- Media Protection and Handling (Standard)

REFERENCES

- NIST SP 800-34 Contingency Planning Guide
- NIST SP 800-12 (chapters 11 & 14) Introduction to Computer Security NIST Handbook
- NIST SP 800-84 Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities
- ITL April 02 Techniques for System and Data Recovery
- ITL June 02 Contingency Planning Guide for IT Systems

Note: PSG number administratively changed from S-08-046.01 on September 1, 2008.